

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-295202

(P2000-295202A)

(43) 公開日 平成12年10月20日 (2000.10.20)

(51) Int.Cl.<sup>7</sup>

識別記号

F I

テーマト\* (参考)

H 0 4 K 1/04

H 0 4 K 1/04

5 C 0 5 9

H 0 4 N 7/167

H 0 4 N 7/167

Z 5 C 0 6 4

// H 0 4 N 7/24

7/13

Z 5 J 1 0 4

審査請求 未請求 請求項の数13 O L (全 11 頁)

(21) 出願番号 特願平11-95756

(22) 出願日 平成11年4月2日 (1999.4.2)

(71) 出願人 000003821

松下電器産業株式会社

大阪府門真市大字門真1006番地

(72) 発明者 櫻井 厚典

大阪府門真市大字門真1006番地 松下電器  
産業株式会社内

(74) 代理人 100099254

弁理士 役 昌明 (外3名)

Fターム(参考) 5C059 KK43 MA00 RB02 RB10 RC35

RD03 RF21 SS02 SS24 UA05

UA38

5C064 CA14 CB01 CB08 CC02 CC04

5J104 AA01 BA03 EA16 NA02 NA35

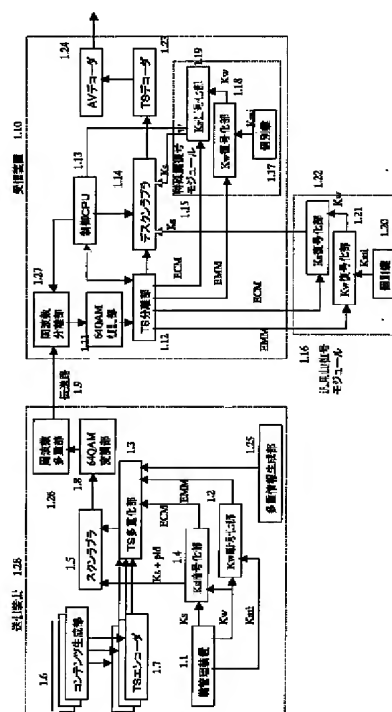
NA37 PA05 PA06

(54) 【発明の名称】 限定受信システム

(57) 【要約】

【課題】 複数のスクランブルされたチャンネルの選択を切り替える時に選択したチャンネルのストリームを短時間でデスクランブルする限定受信システムを提供する。

【解決手段】 送信装置は各チャンネル共通のスクランブル鍵を用いて共通情報を送信し、受信装置は、汎用鍵復号モジュール116と特殊鍵復号モジュール115との2種類の復号手段を持つ。特殊鍵復号モジュールは現在受信中のチャンネルを直接検知する手段113を持ち、また、チャンネルを変更しても前回受信したスクランブル鍵を保持する。受信装置では、特殊鍵復号モジュールを用いて復号する場合、チャンネルを変更しても、そのチャンネルの視聴権がある場合には新たな共通情報の受信を待たずに、チャンネル変更前から保持されたスクランブル鍵を用いてコンテンツストリームをデスクランブルする。



## 【特許請求の範囲】

【請求項1】 複数のチャンネルデータをスクランブルするための鍵データを生成する鍵生成手段と、前記鍵データを用いてチャンネルデータをスクランブルするスクランブル手段とを具備する送信装置と、複数のチャンネルの中から選択した任意のチャンネルを前記鍵データを用いてデスクランブルするデスクランブル手段を具備する受信装置とから成る限定受信システムにおいて、送信装置が、複数のチャンネルを共通の鍵データを用いてスクランブルし、受信装置が、前記共通の鍵データを保持する鍵保持手段を備え、いずれのチャンネルを選局した場合でも前記鍵保持手段に保持された共通の鍵データを用いてデスクランブルすることを特徴とする限定受信システム。

【請求項2】 前記送信装置は、鍵データを格納する関連情報の中に前記共通の鍵データを含めて送信し、前記受信装置は、前記関連情報から取得した前記共通の鍵データを前記鍵保持手段で保持することを特徴とする請求項1に記載の限定受信システム。

【請求項3】 前記送信装置は、鍵データを格納した関連情報に前記鍵データが共通の鍵データであるか否かを示す識別情報を含めて送信し、前記受信装置は、共通の鍵データを示す識別情報が含まれた関連情報から前記鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに前記関連情報から鍵データを取得する汎用鍵復号モジュールとを具備し、前記関連情報に共通の鍵データを示す識別情報が含まれているときは、前記特殊鍵復号モジュールによって取得され、前記鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、前記関連情報に共通の鍵データを示す識別情報が含まれていないときは、前記汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルすることを特徴とする請求項2に記載の限定受信システム。

【請求項4】 前記送信装置は、鍵データを格納した関連情報を送信し、前記受信装置は、前記関連情報から前記鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに前記関連情報から鍵データを取得する、実装可能な汎用鍵復号モジュールと、前記汎用鍵復号モジュールの実装の有無を検出する検出手段とを具備し、前記検出手段が、前記汎用鍵復号モジュールの実装を検出していないときは、前記特殊鍵復号モジュールによって取得され、前記鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、前記検出手段が、前記汎用鍵復号モジュールの実装を検出しているときは、前記汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルすることを特徴とする請求項2に記載の限定受信システム。

【請求項5】 前記受信装置の受信チャンネルが変更さ

れた場合に、前記特殊鍵復号モジュールは、現在受信中のチャンネルに関する情報を受けて、視聴の可否を判断することを特徴とする請求項3または4に記載の限定受信システム。

【請求項6】 前記受信装置は、受信チャンネルの変更後に受信した前記関連情報に基づいて、視聴の可否を確認し、視聴権が無ければデスクランブルを停止することを特徴とする請求項5に記載の限定受信システム。

【請求項7】 前記送信装置は、前記関連情報に番組識別情報を含めて送信し、前記特殊鍵復号モジュールを持たずに、前記汎用鍵復号モジュールのみを具備する受信装置は、前記番組識別情報から視聴の可否を判断することを特徴とする請求項3または4に記載の限定受信システム。

【請求項8】 前記汎用鍵復号モジュールが、ICカードで構成され、前記受信装置は、前記ICカードを挿入するスロットを具備することを特徴とする請求項3、4または7に記載の限定受信システム。

【請求項9】 前記受信装置は、プログラムダウンロード手段を備え、前記送信装置からのダウンロードにより前記特殊鍵復号モジュールを置き換えることを特徴とする請求項3、4、5または7に記載の限定受信システム。

【請求項10】 前記特殊鍵復号モジュールと受信装置のデスクランブラとがPCMCIAカードに実装され、前記受信装置は、前記PCMCIAカードのスロットを具備することを特徴とする請求項3または4に記載の限定受信システム。

【請求項11】 前記送信装置は、前記共通の鍵データを格納した関連情報にバージョン情報を含めて送信し、前記受信装置は、前記バージョン番号が更新されるまで、前記鍵保持手段で保持された同一の共通の鍵データを用いてデスクランブルを続けることを特徴とする請求項2に記載の限定受信システム。

【請求項12】 前記送信装置は、前記共通の鍵データを格納した関連情報に複数種類のスクランブル鍵を含めて送信し、前記受信装置は、前記複数種類のスクランブル鍵を前記鍵保持手段で保持し、コンテンツデータパケットの非スクランブル部の情報からどのスクランブル鍵が用いられているかを識別して、デスクランブルに用いるスクランブル鍵を選択することを特徴とする請求項2に記載の限定受信システム。

【請求項13】 前記受信装置は、番組多重情報を保持する番組多重情報保持手段を備え、番組多重情報が更新された時以外は、前記番組多重情報保持手段に保持された番組多重情報を基に選局することを特徴とする請求項2に記載の限定受信システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明は、ケーブルテレビ、

衛星放送、地上放送等において、番組をスクランブルして放送し、視聴権を持つ場合にのみデスクランブルを可能にする限定受信システムに関し、特に、チャンネルを切り替えたときに、迅速にデスクランブルが開始できるようにしたものである。

#### 【0002】

【従来の技術】従来の標準的な限定受信方法である MPEG2 SYSTEMS (ISO/IEC13818-1) では、送出側は、映像、データ等のコンテンツをスクランブル鍵  $K_s$  でスクランブルして送信し、また、このスクランブル鍵  $K_s$  を ECM (Entitlement Control Messages: 共通情報) に格納した後、この共通情報 ECM をワーク鍵  $K_w$  で暗号化して送信する。また、このワーク鍵  $K_w$  は、事前に、EMM (Entitlement Management Messages: 個別情報) に格納した後、 $K_{mi}$  で暗号化して送信される。

【0003】一方、受信側では、暗号化された個別情報 EMM を受信すると、あらかじめ持っている個別鍵  $K_{mi}$  で復号化し、EMM からワーク鍵  $K_w$  を取り出して保持する。また、暗号化された共通情報 ECM と、スクランブルされたコンテンツストリームとを受信すると、ECM をワーク鍵  $K_w$  で復号化して ECM からスクランブル鍵  $K_s$  を取り出し、スクランブルされているコンテンツストリームを、取り出した  $K_s$  を用いてデスクランブルする。デスクランブルされた映像は、AV デコードによって視聴可能なアナログ信号に変換される。

#### 【0004】

【発明が解決しようとする課題】従来の標準的な限定受信方式では、チャンネルを切り替えた場合に、その都度、新たに ECM からスクランブル鍵  $K_s$  を取得しているため、デスクランブルが再開されるまでに時間が掛かるという問題があった。

【0005】また、この問題を避けるために、送信側で ECM を用いる標準的な方法では無く、チャンネル視聴可否を直接制御する独自の方式を採ると、受信側では、送信側の方式に合わせた独自方式の受信装置でしか対応することができなくなり、ECM を用いる標準的な限定受信方式の受信装置では限定受信ができなくなるという問題が生じる。

【0006】本発明は、こうした問題点を解決するものであり、チャンネルを切り替えた場合のデスクランブルを迅速に行うことができ、また、ECM を用いる標準的な限定受信方式の受信装置でも限定受信処理自体は支障なく行うことができる限定受信システムを提供することを目的としている。

#### 【0007】

【課題を解決するための手段】そこで、本発明の限定受信システムでは、送信装置が、複数のチャンネルを共通の鍵データを用いてスクランブルし、受信装置は、この共通の鍵データを保持する鍵保持手段を具備し、いずれ

のチャンネルが選局された場合でも鍵保持手段に保持された共通の鍵データを用いてデスクランブルする。

【0008】そのため、受信装置では、受信中のチャンネルが、別の視聴権のあるチャンネルに切り替えられた場合でも、共通情報 ECM の受信を待たずに、保持しているスクランブル鍵を用いて、切り替えたチャンネルのデータをデスクランブルすることができる。

#### 【0009】

【発明の実施の形態】本発明の請求項 1 に記載の発明は、複数のチャンネルデータをスクランブルするための鍵データを生成する鍵生成手段と、鍵データを用いてチャンネルデータをスクランブルするスクランブル手段とを具備する送信装置と、複数のチャンネルの中から選択した任意のチャンネルをこの鍵データを用いてデスクランブルするデスクランブル手段を具備する受信装置とから成る限定受信システムにおいて、送信装置が、複数のチャンネルを共通の鍵データを用いてスクランブルし、受信装置が、この共通の鍵データを保持する鍵保持手段を備え、いずれのチャンネルを選局した場合でも鍵保持手段に保持された共通の鍵データを用いてデスクランブルするようにしたものであり、受信装置では、受信中のチャンネルを別の視聴権のあるチャンネルに切り替える場合に、共通情報 ECM の受信を待たずに、そのチャンネルのデータをデスクランブルし、視聴が可能になる。

【0010】請求項 2 に記載の発明は、送信装置が、鍵データを格納する関連情報の中に共通の鍵データを含めて送信し、受信装置は、関連情報から取得した共通の鍵データを鍵保持手段で保持するようにしたものであり、送信装置は、各チャンネルデータを共通の鍵データを用いてスクランブルする場合には、その鍵データを関連情報（即ち、個別情報 EMM 及び共通情報 ECM）で送信し、受信装置は、関連情報から取得した共通の鍵データを保持して各チャンネルのデスクランブルに使用する。

【0011】請求項 3 に記載の発明は、送信装置が、鍵データを格納した関連情報に鍵データが共通の鍵データであるか否かを示す識別情報を含めて送信し、受信装置は、共通の鍵データを示す識別情報が含まれた関連情報から鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに関連情報から鍵データを取得する汎用鍵復号モジュールとを具備し、関連情報に共通の鍵データを示す識別情報が含まれているときは、特殊鍵復号モジュールによって取得され、鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、関連情報に共通の鍵データを示す識別情報が含まれていないときは、汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルするようにしたものであり、一台の受信装置で、請求項 1 の限定受信方式と従来の一般的な限定受信方式の二通りの方式に対応することができる。

【0012】請求項4に記載の発明は、送信装置が、鍵データを格納した関連情報を送信し、受信装置は、関連情報から鍵保持手段で保持される共通の鍵データを取得する特殊鍵復号モジュールと、受信チャンネルが変わるごとに関連情報から鍵データを取得する、実装可能な汎用鍵復号モジュールと、汎用鍵復号モジュールの実装の有無を検出する検出手段とを具備し、検出手段が、汎用鍵復号モジュールの実装を検出していないときは、特殊鍵復号モジュールによって取得され、鍵保持手段で保持された共通の鍵データを用いてデスクランブルし、検出手段が、汎用鍵復号モジュールの実装を検出しているときは、汎用鍵復号モジュールによって取得された鍵データを用いてデスクランブルするようにしたものであり、一台の受信装置で、請求項1の限定受信方式と従来の一般的な限定受信方式の二通りの方式に対応することができる。

【0013】請求項5に記載の発明は、受信装置の受信チャンネルが変更された場合に、特殊鍵復号モジュールは、現在受信中のチャンネルに関する情報を受けて、視聴の可否を判断するようにしたものであり、切り替えたチャンネルが視聴権を有するチャンネルであるかどうかを判断し、視聴権を有するチャンネルである場合に、共通の鍵データによるデスクランブルが開始される。

【0014】請求項6に記載の発明は、受信装置が、受信チャンネルの変更後に受信した関連情報に基づいて、視聴の可否を確認し、視聴権が無ければデスクランブルを停止するようにしたものであり、関連情報の番組情報を照合して、視聴権が無い場合にはデスクランブルを停止することにより、限定受信のセキュリティを向上することが可能となる。

【0015】請求項7に記載の発明は、送信装置が、関連情報に番組識別情報を含めて送信し、特殊鍵復号モジュールを持たずに、汎用鍵復号モジュールのみを具備する受信装置は、番組識別情報から視聴の可否を判断するようにしたものであり、請求項1の限定受信方式を採りながら、従来の限定受信方式の受信装置でも、限定受信処理を行うことができる。

【0016】請求項8に記載の発明は、汎用鍵復号モジュールが、ICカードで構成され、受信装置は、このICカードを挿入するスロットを具備するようにしたものであり、一般的な限定受信モジュールを汎用鍵復号モジュールとして用いることが可能になる。

【0017】請求項9に記載の発明は、受信装置が、プログラムダウンロード手段を備え、送信装置からのダウンロードにより特殊鍵復号モジュールを置き換えるようにしたものであり、特殊鍵限定受信方式のアルゴリズムを必要に応じて変更することが可能となる。

【0018】請求項10に記載の発明は、特殊鍵復号モジュールと受信装置のデスクランブラとがPCMCIAカードに実装され、受信装置は、このPCMCIAカー

ドのスロットを具備するようにしたものであり、特殊鍵限定受信方式のアルゴリズムを必要に応じて変更することが可能となる。

【0019】請求項11に記載の発明は、送信装置が、共通の鍵データを格納した関連情報にバージョン情報を含めて送信し、受信装置は、バージョン番号が更新されるまで、鍵保持手段で保持された同一の共通の鍵データを用いてデスクランブルを続けるようにしたものであり、共通情報ECMの内容が変更されるまで関連情報を復号する必要が無くなり、受信装置の処理負荷を低減することが可能となる。

【0020】請求項12に記載の発明は、送信装置が、共通の鍵データを格納した関連情報に複数種類のスクランブル鍵を含めて送信し、受信装置は、複数種類のスクランブル鍵を鍵保持手段で保持し、コンテンツデータパケットの非スクランブル部の情報からどのスクランブル鍵が用いられているかを識別して、デスクランブルに用いるスクランブル鍵を選択するようにしたものであり、スクランブル鍵の更新と、共通情報の更新のタイミングとを厳密に同期を取る必要が無くなる。

【0021】請求項13に記載の発明は、受信装置が、番組多重情報を保持する番組多重情報保持手段を備え、番組多重情報が更新された時以外は、番組多重情報保持手段に保持された番組多重情報を基に選局するようにしたものであり、PSIの受信を待たずに選局及び関連情報の受信が可能となりチャンネル変更時のレスポンスがさらに向上する。

【0022】以下、本発明の実施の形態について、図1～図6を用いて説明する。

【0023】実施形態のシステムにおいて、送信装置128は、スクランブル鍵Ks、ワーク鍵Kw及び個別鍵Kmiを生成管理する鍵管理装置11と、ワーク鍵Kwを格納した個別情報EMMをKmiで暗号化するKw暗号化部12と、スクランブル鍵Ksを格納した共通情報ECMをKwで暗号化するKs暗号化部14と、映像、データ等のコンテンツを生成するコンテンツ生成部16と、コンテンツをMPEG2 SYSTEMS (ISO/IEC13818-1)のTSパケット (Transport Stream Packet) のデータフォーマットに変換するTSエンコーダ17と、MPEG2 SYSTEMSのPSI (Program Specific Information) をチャンネル、番組の情報に合わせて生成する多重情報生成部125と、個別情報EMM、共通情報ECM、トランスポートストリーム及びPSIをMPEG2 SYSTEMS (180/IEC13818-1)の規定通りに多重化するTS多重化部13と、TS多重化部13で多重化されたデータの中からコンテンツストリームのみをスクランブル鍵Ksでスクランブルするスクランブラ15と、送信データを64Q変調する64Q変調部18と、変調した信号を周波数多重する周波数多重部126とを備えている。

【0024】一方、受信装置110は、伝送路19より受信

した信号を周波数分離する周波数分離部127と、受信信号を64QAM復調する64QAM復調部111と、受信信号からPSI、映像ストリーム、共通情報ECM、個別情報EMM等を分離するTS分離部112と、選局されたチャンネルの映像ストリームをKsを用いてデスクランブルするデスクランブラ114と、デスクランブルされたストリームをコンテンツストリームの形式に変換するTSデコード123と、コンテンツストリームを視聴可能なアナログ信号に変換するAVデコード124と、PSI情報に基づいてフィルタリングすべきProgram-IDをTS分離部112やデスクランブラ114等に伝える制御CPU113と、Ksを復号化する特殊鍵復号モジュール115と、ICカードで構成される、Ksを復号化する汎用鍵復号モジュール116とを備えている。

【0025】特殊鍵復号モジュール115は、送信側が複数のチャンネルに共通のKsを用いる場合に、そのKsの復号化を行うものであり、EMMを、あらかじめ持っている個別鍵Kmi117で復号化してKwを取り出すKw復号化部118と、ECMをKwで復号化してKsを取り出すKs復号化部119とを備えており、このKs復号化部119には制御CPU113から選局したチャンネルが伝えられる。

【0026】また、ICカードで構成される汎用鍵復号モジュール116は、送信側が複数のチャンネルに共通のKsを用いない場合に、そのKsの復号化を行うものであり、特殊鍵復号モジュール115と同様に、EMMを個別鍵Kmi120で復号化してKwを取り出すKw復号化部121と、ECMをKwで復号化してKsを取り出すKs復号化部122とを備えている。この汎用鍵復号モジュール116は、ICカードを取り替えることによって交換可能である。

【0027】まず、このシステムでの送受信の概要に関して説明する。

【0028】送出側では、鍵管理装置11がワーク鍵Kwを生成し、これを個別情報EMMに格納した後に、Kw暗号化部12が、個別情報EMMをあらかじめ鍵管理装置11から受け取っているKmiを用いて暗号化し、暗号化された個別情報としてTS多重化部13に送出する。TSとはMPEG2SYSTEMS (ISO/IEC13818-1)におけるTransport Stream Packetのことである。

【0029】また、スクランブル鍵Ksは、鍵管理装置11が生成し共通情報ECMに格納した後に、Ks暗号化部14が、共通情報ECMをあらかじめ鍵管理装置11から受け取っているKwを用いて暗号化し、暗号化された共通情報としてTS多重化部13に送出する。

【0030】また、映像、データ等のコンテンツは、コンテンツ生成部16よりTSエンコード17に送られ、MPEG2SYSTEMS (ISO/IEC13818-1)におけるTSパケット (Transport Stream Packet) のデータフォーマットに変換される。TS化された映像情報等のコンテ

ンツデータはTS多重化部13に送られる。

【0031】また、マルチプログラム構成の場合は、コンテンツデータは複数のコンテンツ生成部からそれぞれのTSエンコードに送られ、TSエンコード17はコンテンツデータをTSパケット化しTS多重化部13に送る。

【0032】また、多重情報生成部125では、MPEG2SYSTEMSのPSIをチャンネル、番組の情報に合わせて生成し、TS多重化部13に送る。

【0033】TS多重化部13に送られた個別情報EMM、共通情報ECM、コンテンツストリーム及びPSIは、MPEG2SYSTEMS (180/IEC13818-1)での規定通り多重化され、スクランブラ15に送られる。スクランブラ15では、Ks暗号化部14から渡されたスクランブル鍵Ksを用いてコンテンツストリームのみをスクランブルし、スクランブルされたトランスポートストリームを64QAM変調部18に送り64QAM変調する。さらに他に64QAM変調された信号とともに周波数多重部126において周波数多重を行い、伝送路19に送出する。

【0034】一方、受信装置110では、伝送路19より受信した信号を周波数分離部127で周波数分離し、64QAM復調部111で復調し、復調された信号がTS分離部112で分離される。

【0035】制御CPU113は、受信装置操作部で選局したチャンネルのPSI情報を基にフィルタリングすべきProgram-IDを取得してTS分離部112に伝達し、それによって、TS分離部112では、該当チャンネルの復調されたトランスポートストリームを関連情報 (以下、共通情報ECM、個別情報EMMの総称とする) と、映像ストリーム等とに分離することが可能になる。また、制御CPU113は、デスクランブルするProgram-IDをデスクランブラ114に設定し、選局したチャンネルをKs復号化部119に設定する。

【0036】また、受信装置110は、受信装置内回路基板に実装された特殊鍵復号モジュール115と、ICカードで構成される汎用鍵復号モジュール116とを持ち、TS分離部112により分離された関連情報は、特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれかに送られ、そこで、コンテンツをデスクランブルするためのスクランブル鍵Ksが取り出される。

【0037】例えば、特殊鍵復号モジュール115を用いた場合では、TS分離部112により分離された個別情報EMMは、Kw復号部118で、あらかじめ持っている個別鍵Kmi117を使って復号され、個別情報EMM内に格納されたワーク鍵Kwが取り出されてKs復号部119に設定される。また、TS分離部112により分離された共通情報ECMは、Ks復号部119で、先に取り出されたワーク鍵Kwを使って復号され、共通情報ECM内に格納されたKsが取り出されてデスクランブラ114に設定される。

【0038】TS分離部112で分離された映像などのコ

ンテンツストリームは、デスクランブラ114において、セットされたスクランブル鍵Ksを使ってデスクランブルされ、TSデコーダ123に送られてコンテンツストリームの形式に変換され、さらに映像はAVデコーダ124により視聴可能なアナログ信号に変換される。

【0039】以上が送受信方法の概略であるが、次に共通情報ECM及び個別情報EMMの具体内容を示しながら、より詳細な送受信方法について述べる。

【0040】送信側の処理として、まず、鍵管理装置11は、図3に示すデータフォーマットの個別情報EMMを各受信装置毎に生成する。また、Kw暗号化部12は、図3に示すデータフォーマットの暗号部のみを個別鍵Kmiで暗号化し、TSパケット化してTS多重化部13を通して、番組の送信に先立ってあらかじめ送信する。

【0041】個別情報EMMの各フィールドの意味は次のとおりである。非暗号部のモジュール識別フラグには特殊鍵復号モジュール115または汎用鍵復号モジュール116のどちらを用いるかを識別する情報が入る。ここでは特殊鍵復号モジュール115を示す識別情報を入れる。受信装置IDには受信装置を識別するIDを入れる。バージョン情報には受信装置ID毎に個別情報のバージョン情報を入れる。すなわち送出側では、受信装置に個別情報を送る際に、受信装置ID毎の個別情報を更新する毎にバージョン情報の値をインクリメントして送出する。暗号化されるフィールドには、ワーク鍵と、該当する受信装置IDに対して付与する個別オーソライズ情報とを入れる。

【0042】また、鍵管理装置11は、図2に示すデータフォーマットの共通情報ECMを各チャンネル毎に生成する。Ks暗号化部14は、ワーク鍵Kwを使って図2に示すデータフォーマットの暗号部のみを暗号化し、TSパケット化してTS多重化部13を通して送信する。

【0043】共通情報ECMの各フィールドの意味は次のとおりである。前述の個別情報EMMと同様に、非暗号化部にモジュール識別フラグとバージョン情報とを付与する。ただし、バージョン情報は、暗号部の番組識別情報などスクランブル鍵以外が更新された場合にのみ、全チャンネルの共通情報のバージョン情報が一斉に更新される。通常はバージョン情報には番号を設定し、更新毎にインクリメントして設定する。

【0044】また、暗号部には、スクランブル鍵と番組識別情報等とを入れる。スクランブル鍵は、各チャンネル共通の鍵を2種類スクランブル鍵1、スクランブル鍵2として設定する。ある一時点で使われているスクランブル鍵がいずれであるかという情報はコンテンツストリームのTSパケットヘッダにおけるtransport-scrambling-controlにて設定する。例えば、スクランブル鍵Ksの更新は、スクランブル鍵1と、スクランブル鍵2とを互いに交代に1分ごとに行う。

【0045】Ks暗号化部14は、スクランブラ15に対し、スクランブル対象のコンテンツストリーム全てに共通にKsを設定する。また、Ks暗号化部14は、それぞれのチャンネル毎に共通のスクランブル鍵をセットした共通情報ECMを生成し送出する。

【0046】一方、受信装置110では、関連情報を受信した場合に、TS分離部112において関連情報のモジュール識別フラグの情報を参照し、そのフラグに応じて、特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれかに、その関連情報を振り分けて送る。

【0047】特殊鍵復号モジュール115に送られた個別情報EMMは、Kw復号化部118において、受信装置IDが該当受信装置と一致し、さらにバージョン情報より前回受信した個別情報から更新されていると判断された場合にのみ、個別鍵Kmi 117で復号され、Kwと個別オーソライズ情報とが取り出されてKs復号化部119に設定される。なお、受信装置IDによるフィルタリングはTS分離部112であらかじめ行っても良い。

【0048】また、TS分離部112において、共通情報ECMを受信し、モジュール識別フラグに基づいて特殊鍵復号モジュール115に振り分ける場合には、まず、現在受信中の共通情報ECMが特殊鍵復号モジュール115で復号処理されていることを制御CPU113に通知する。次に、共通情報ECMが入力したKs復号化部119では、バージョン情報が前回受信した共通情報から更新されていると判断した場合にのみ、そのECMを先にセットされたワーク鍵Kwを用いて復号する。そして、復号したデータから個別オーソライズ情報と番組識別情報とを比較し、チャンネル視聴権がある場合にのみ、スクランブル鍵1とスクランブル鍵2とを取り出し、両方の鍵をデスクランブラ114に設定する。

【0049】デスクランブラ114は、コンテンツストリームのTSパケットヘッダにおけるtransport-scrambling-controlを参照して、スクランブル鍵1またはスクランブル鍵2のいずれを用いてデスクランブルするかをTSパケット毎に選択する。また、これらの鍵は、後述するチャンネル変更時の処理のためにKs復号化部119で保持される。

【0050】次に、受信装置操作部でチャンネルを変更した時の処理について説明する。

【0051】チャンネルが変更されると、制御CPU113は、現在使われている復号モジュールが特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれであるかを前述の通知情報から判断し、特殊鍵復号モジュール115を使用している場合には、制御CPU113からKs復号化部119に直接、変更されたチャンネル情報を通知する。

【0052】Ks復号化部119は、通知されたチャンネルが視聴権のあるチャンネルであるかどうかを個別オーソライズ情報から判断し、視聴権がある場合には、既に



保持しているスクランブル鍵K<sub>s</sub>をデスクランブラ114に設定する。スクランブル鍵がK<sub>s</sub>復号化部119に設定されていない場合には、新たな共通情報ECMを受信し、復号化してスクランブル鍵K<sub>s</sub>を取り出す。チャンネルを変更後も共通情報ECMを受信して番組識別情報を取り出し、個別オーソライズ情報と比較参照した結果、視聴権が無ければデスクランブラ114へのK<sub>s</sub>への供給を停止する。

【0053】なお、受信装置110において、チャンネル変更後に新たに共通情報から受信チャンネルの確認検証を行わない場合には、共通情報内に番組識別情報は不要である。この場合は共通情報自体も各チャンネルで共通にすることが可能である。

【0054】また、受信装置110において、特殊鍵復号モジュール115とデスクランブラ114とをフラッシュROMに実装し、送信装置からのデータダウンロードにより特殊鍵復号モジュール115の復号方式、アルゴリズム、デスクランブル方式を置き換えるようにしても良い。

【0055】また、特殊鍵復号モジュール115とデスクランブラ114とをPCMCIAカードに実装し、受信装置110にはPCMCIAスロットを設け、PCMCIAカードを入れ替えることにより特殊鍵復号モジュール115の復号方式、アルゴリズム、デスクランブル方式を置き換えるようにしても良い。

【0056】次に、特殊鍵復号モジュールを持たず、汎用鍵復号モジュール116のみを持つ受信装置において、特殊鍵復号モジュール用の関連情報を用いて受信する場合について述べる。これは送信側は本方式のシステムを用い、受信側はICカードなどによってCA方式を変更することができる機能のみ持った従来の汎用的な受信装置である場合を想定しており、本限定受信方式は、こうした受信装置においても、チャンネル変更時の高速化の効果は得られないものの、限定受信処理自体は問題なく行われることを説明する。

【0057】この受信装置の構成図を図6に示す。図1の受信装置に比べて、特殊鍵復号モジュール115が無い点だけが相違している。

【0058】この従来の汎用的な受信装置では、特に関連情報のモジュール識別フラグの情報を参照する仕組みは無いので、TS分離部112は、個別情報EMMに含まれる受信装置IDが該当受信装置と一致し、さらに、そのバージョン情報より前回受信した個別情報から更新されていると判断した場合には、全ての個別情報EMMを汎用鍵復号モジュール116に送る。

【0059】汎用鍵復号モジュール116では、K<sub>w</sub>復号化部121が、あらかじめ持っている個別鍵K<sub>mi</sub> 120を用いてEMMを復号し、K<sub>w</sub>と個別オーソライズ情報とを取り出してK<sub>s</sub>復号化部122に設定する。また、共通情報ECMに関しては、K<sub>s</sub>復号化部122が、先に設定されたワーク鍵K<sub>w</sub>を用いて復号し、復号したデータから

個別オーソライズ情報と番組識別情報とを比較してチャンネル視聴権がある場合にのみ、スクランブル鍵1とスクランブル鍵2とを取り出し、K<sub>s</sub>復号化部121に保持し、また両方の鍵をデスクランブラ114に設定する。

【0060】デスクランブラ114は、コンテンツストリームのTSパケットヘッダにおけるtransport\_scrambling\_controlを参照して、スクランブル鍵1またはスクランブル鍵2のいずれを用いてデスクランブルするかをTSパケット毎に選択する。

【0061】また、受信装置操作部によりチャンネルが変更された時には、該当するチャンネルで新たな共通情報の受信を待ち、それを受信すると復号化してスクランブル鍵K<sub>s</sub>を取り出し、コンテンツストリームをデスクランブルする。すなわち、特殊鍵復号モジュール115を有する本システム用の受信装置のように、蓄積されたスクランブル鍵を用いることは、行われない。

【0062】次に、図1の受信装置110において、汎用鍵復号モジュール116を用いて処理する場合について述べる。これは、本発明の受信装置が、従来の一般的なCA方式による受信を行う場合を想定している。

【0063】この場合、送信側は、図5に示すデータフォーマットの個別情報EMMを送信し、また、図4に示すデータフォーマットの共通情報ECMを送信する。これらの非暗号部のモジュール識別フラグには、汎用鍵復号モジュールの使用を指定する情報が入る。また、EMMの暗号化されるフィールドには、ワーク鍵と、該当する受信装置IDに対応する個別ティア情報とが入り、ECMの暗号化されるデータフィールドにはスクランブラ鍵と番組ティア情報とが入る。

【0064】受信装置は、ICカードスロットを備え、汎用鍵復号モジュール116を組み込んだICカードを挿入できる構成を備えている。

【0065】受信装置が図5に示す個別情報EMMを受信した場合に、TS分離部112は、関連情報のモジュール識別フラグの情報を参照し、そこに汎用鍵復号モジュール116の利用を求す情報が付加されているために、その個別情報をICカードの汎用鍵復号モジュール116に振り分けて送る。その後の処理は、特殊鍵復号モジュール115における処理と同じであり、K<sub>w</sub>復号化部121は、K<sub>w</sub>と個別ティア情報とを取り出してK<sub>s</sub>復号化部122に設定する。

【0066】また、TS分離部112が図4に示す共通情報ECMを受信した場合には、モジュール識別フラグに基づいて汎用鍵復号モジュール116に振り分ける前に、現在受信中の共通情報ECMが汎用鍵復号モジュール116で復号処理されていることを制御CPU113に通知する。また、共通情報ECMが入力したK<sub>s</sub>復号化部122は、特殊鍵復号モジュール115での処理と同様に、バージョン情報が前回受信した共通情報から更新されている

場合に、そのECMをワーク鍵Kwで復号し、復号したデータから個別ティア情報と番組ティア情報とを比較し、チャンネル視聴権がある場合にスクランブル鍵を取り出す。ただし、取り出したスクランブル鍵は、Ks復号化部121に保持せずに、デスクランブラ114に設定する。

【0067】次に、チャンネルが変更されると、制御CPU113は、現在使われている復号モジュールが特殊鍵復号モジュール115または汎用鍵復号モジュール116のいずれであるかを前述の通知情報から判断し、汎用鍵復号モジュール116の場合には、何も行わない。

【0068】受信装置110は、新たな共通情報ECMの受信を待ち、受信すると、汎用鍵復号モジュール116のKs復号化部122がワーク鍵で復号化した後、番組ティア情報と個別ティア情報との組み合わせによって視聴権の可否を判断し、視聴権がある場合には共通情報内のスクランブル鍵Ksをスクランブラ114に設定する。

【0069】なお、チャンネル選択時に多重情報から該当のチャンネルのコンテンツストリームを取り出すために、チャンネル選局の都度、PSI情報を取得して取り出すが、チャンネル選局から実際にコンテンツストリームを得るまでの時間をさらに短縮するために、受信装置にPSI情報をあらかじめ蓄積し、そのPSI情報を基に該当チャンネルのコンテンツストリーム及び関連情報の分離を行うようにしても良い。

【0070】また、本実施の形態では、受信装置は関連情報のモジュール識別フラグを参照することにより、関連情報を特殊鍵復号モジュール115に送るか汎用鍵復号モジュール116に送るかを判断しているが、例えば、汎用鍵復号モジュール115をICカードに実装している場合には、受信装置のICカードスロットに物理的なICカード挿入検出手段を設け、ICカードが挿入されている場合は、ICカード中の汎用鍵復号モジュールに関連情報を送り、ICカードが挿入されていない場合には、受信装置内の特殊鍵復号モジュール115に関連情報を送付することによって関連情報の振り分けを行っても同様の効果が得られる。その場合には、関連情報にモジュール識別フラグは必要ない。

【0071】

【発明の効果】以上の説明から明らかなように、本発明の限定受信システムでは、受信装置で受信しているチャンネルを、別の視聴権のあるチャンネルに切り替えた場合に、そのチャンネルのデータを迅速にデスクランブルすることができる。

【0072】また、一台の受信装置で、本発明の限定受信方式にも、従来の一般的な限定受信方式にも対応することができる。

【0073】また、従来の限定受信方式の受信装置であっても、チャンネル切り替え時の高速デスクランブルの効果は得られないが、限定受信処理自体は支障なく行う

ことができる。

【0074】また、プログラムダウンロード手段を設けた受信装置や、特殊鍵復号モジュールとデスクランブラとをPCMCIAカードに実装した受信装置では、共通の鍵データを用いる特殊鍵限定受信方式のアルゴリズムを必要に応じて変更することが可能である。

【0075】また、共通の鍵データを送信する関連情報にバージョン番号を含めることにより、受信装置では、バージョン番号が更新されるまでは関連情報の復号が不要になり、受信装置の処理負荷を低減することができる。

【0076】また、受信装置で複数の共通の鍵データを保持し、コンテンツデータパケットの非スクランブル部の情報を基に、デスクランブルに用いるスクランブル鍵を選択する場合には、スクランブル鍵の更新と、共通情報の更新のタイミングとを厳密に同期を取る必要が無くなる。

【0077】また、受信装置で番組多重情報を保持し、この番組多重情報を基に選局するようにしたものでは、PSIの受信を待たずに選局及び関連情報の受信が可能となりチャンネル変更時のレスポンスをさらに向上することができる。

【図面の簡単な説明】

【図1】本発明の実施形態における限定受信システムの送信装置及び受信装置の構成を示すブロック図、

【図2】本発明の実施形態の特殊鍵モジュール用共通情報のデータフォーマットを示す図、

【図3】本発明の実施形態の特殊鍵モジュール用個別情報のデータフォーマットを示す図、

【図4】本発明の実施形態の汎用鍵モジュール用共通情報のデータフォーマットを示す図、

【図5】本発明の実施形態の汎用鍵モジュール用個別情報のデータフォーマットを示す図、

【図6】本発明の実施形態の限定受信システムに適用可能な従来の汎用的な受信装置の構成を示すブロック図である。

【符号の説明】

- 11 鍵管理装置
- 12 Kw暗号化部
- 13 TS多重化部
- 14 Ks暗号化部
- 15 スクランブラ
- 16 コンテンツ生成部
- 17 TSエンコーダ
- 18 64Q変調部
- 19 伝送路
- 110 受信装置
- 111 64QAM復調部
- 112 TS分離部
- 113 制御CPU



- |                 |             |
|-----------------|-------------|
| 114 デスクランブラ     | 123 TSデコーダ  |
| 115 特殊鍵復号モジュール  | 124 AVデコーダ  |
| 116 汎用鍵復号モジュール  | 125 多重情報生成部 |
| 117、120 個別鍵Km i | 126 周波数多重部  |
| 118、121 Kw復号化部  | 127 周波数分離部  |
| 119、122 Ks復号化部  | 128 送信装置    |

【図2】

非暗号部			ワーク鍵による暗号部			
モジュール識別フラグ	バージョン情報	その他	スクランブル鍵1	スクランブル鍵2	番組識別情報	その他

【図3】

非暗号部				個別鍵による暗号部		
モジュール識別フラグ	受信装置ID	バージョン情報	その他	ワーク鍵	個別オーソライズ情報	その他

【図4】

非暗号部			ワーク鍵による暗号部			
モジュール識別フラグ	バージョン情報	その他	スクランブル鍵1	スクランブル鍵2	番組ティア情報	その他

【図5】

非暗号部				個別鍵による暗号部		
モジュール識別フラグ	受信装置ID	バージョン情報	その他	ワーク鍵	個別ティア情報	その他



【図6】

